REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application.

35 U.S.C. § 102

Claims 1-37 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,044,388 to DeBellis et al. (hereinafter "DeBellis"). Applicant respectfully submits that claims 1-37 are not anticipated by DeBellis.

DeBellis discloses generating a pseudorandom number by "concatenating a time-dependent value (generated by a real-time counter) with a secret value and passing the concatenation result through a one-way hash function to generate a hash value from which a random number is generated." (col. 4, line 66 – col. 5, line 5). Applicant submits that the DeBellis reference fails to disclose the elements of pending claims 1-4, 6-14, 16-32, and 34-37.

Claim 1, as amended, recites:

> A method comprising:
> collecting entropy data, wherein the entropy data includes operating system data;
> storing the entropy data in a nonvolatile memory;
> updating the entropy data stored in the nonvolatile memory with newly collected entropy data; and
> generating a string of random bits from the entropy data stored in the nonvolatile memory.

Applicant submits that DeBellis fails to disclose "collecting entropy data, wherein the entropy data includes operating system data" and "generating a string of random bits from the entropy data...", as recited in claim 1. As mentioned above, DeBellis discloses generating a pseudorandom number using "a time-dependent value (generated by a real-time counter)" and "a secret value". The real-time counter value and the secret value are not operating system data. Further, DeBellis fails to disclose the use of any operating system data to generate a string of random bits. Thus, DeBellis fails to disclose the elements of amended claim 1.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 1 is allowable over DeBellis. Given that claims 2-4 and 6-10 depend from claim 1, Applicant respectfully submits that those claims are likewise allowable over DeBellis for at least the reasons discussed above.

Claim 6 is further allowable because DeBellis fails to disclose "wherein the entropy data is maintained in a protected portion of an operating system kernel", as recited in claim 6. Applicant submits that DeBellis fails to make any reference to storing entropy data in a protected portion of an operating system kernel. Thus, DeBellis fails to disclose this additional element of claim 6.

Claim 7 is further allowable because DeBellis fails to disclose "wherein the entropy data is inaccessible by an application program executing on the system", as recited in claim 7. Applicant submits that DeBellis fails to make any reference to the entropy data being inaccessible by an application program. Thus, DeBellis fails to disclose this additional element of claim 7.

Claim 8 is further allowable because DeBellis fails to disclose "wherein updating the entropy data includes hashing the entropy data stored in the nonvolatile memory with the newly collected entropy data", as recited in claim 8. Applicant submits that DeBellis fails to make any reference to hashing the existing entropy data with the new entropy data to update the entropy data. Although DeBellis mentions a one-way hash function, DeBellis fails to make any reference to hashing existing entropy data with newly collected entropy data for the purpose of updating the entropy data. Thus, DeBellis fails to disclose this additional element of claim 8.

Claim 11, as amended, recites:

> One or more computer-readable memories containing a computer program that is executable by one or more processors, the computer program causing the one or more processors to:
>
> collect entropy data, wherein the entropy data includes processor data;
>
> store the entropy data in a nonvolatile memory;
>
> update the entropy data stored in the nonvolatile memory with newly collected entropy data; and
>
> generate a string of random bits from the entropy data stored in the nonvolatile memory.

Applicant submits that DeBellis fails to disclose "collecting entropy data, wherein the entropy data includes processor data" and "generating a string of random bits from the entropy data...", as recited in claim 11. As mentioned above, DeBellis discloses generating a pseudorandom number using "a time-dependent value (generated by a real-time counter)" and "a secret value". The real-time counter value and the secret value are <u>not</u> processor data. Further, DeBellis fails to disclose the use of any processor data to generate a string of random bits. Thus, DeBellis fails to disclose the elements of amended claim 11. Accordingly, for at least these reasons, Applicant respectfully submits that claim 11 is allowable over DeBellis.

Claim 12, as amended, recites:

> A method comprising:
> receiving a request for a random number;
> retrieving, from a protected portion of an operating system kernel, entropy data that is regularly updated with newly collected entropy data;
> hashing the entropy data to create random seed data;
> generating a string of random bits from the random seed data; and
> communicating the string of random bits to the requester of the random number.

Applicant submits that DeBellis fails to disclose "retrieving, from a protected portion of an operating system kernel, entropy data that is regularly updated with newly collected entropy data", as recited in claim 12. As mentioned above with respect to claim 6, DeBellis fails to make any reference to storing entropy data in a protected portion of an operating system kernel. Thus, DeBellis fails to disclose the elements of amended claim 12.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 12 is allowable over DeBellis. Given that claims 13-14 and 16-17 depend from claim 12, Applicant respectfully submits that those claims are likewise allowable over DeBellis for at least the reasons discussed above.

Claim 18, as amended, recites a computer program that causes one or more of the processors to "retrieve entropy data from a protected portion of an operating system kernel". As discussed above with respect to claims 6 and 12, DeBellis fails to make any reference to storing or retrieving entropy data in or from a protected portion of an operating system kernel. Thus, DeBellis fails to disclose the elements of amended claim 18. Accordingly, for at least these reasons, Applicant respectfully submits that claim 18 is allowable over DeBellis.

Claim 19 includes "storing the entropy data in a protected portion of an operating system kernel". As discussed above with respect to claims 6 and 12, DeBellis fails to make any reference to storing entropy data in a protected portion of an operating system kernel. Thus, DeBellis fails to disclose the elements of claim 19.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 19 is allowable over DeBellis. Given that claims 20-23 depend from claim 19, Applicant respectfully submits that those claims are likewise allowable over DeBellis for at least the reasons discussed above.

Claim 24, as amended, recites a computer program that causes one or more processors to "store the entropy data in a protected portion of an operating system kernel". As discussed above with respect to claims 6 and 12, DeBellis fails to make any reference to storing entropy data in a protected portion of an operating system kernel. Thus, DeBellis fails to disclose the elements of amended claim 24. Accordingly, for at least these reasons, Applicant respectfully submits that claim 24 is allowable over DeBellis.

Claim 25 includes "wherein the entropy data stored in the nonvolatile memory is updated regularly by hashing the entropy data stored in the nonvolatile memory with newly collected entropy data". As discussed above with respect to claim 8, DeBellis fails to make any reference to hashing the existing entropy data with the new entropy data to update the entropy data. Thus, DeBellis fails to disclose the elements of amended claim 25.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 25 is allowable over DeBellis. Given that claims 26-31 depend from claim

25, Applicant respectfully submits that those claims are likewise allowable over DeBellis for at least the reasons discussed above.

Claim 32, as amended, recites:

> One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:
>
> collect entropy data from multiple sources within a computing system, wherein the entropy data is associated with a state of at least one processor;
>
> store the collected entropy data in a nonvolatile memory;
>
> update the entropy data stored in the nonvolatile memory with newly collected entropy data; and
>
> produce a string of random bits from the entropy data stored in the nonvolatile memory.

Applicant submits that DeBellis fails to disclose "collect entropy data from multiple sources within a computing system, wherein the entropy data is associated with a state of at least one processor", as recited in claim 32. As mentioned above, DeBellis discloses generating a pseudorandom number using "a time-dependent value (generated by a real-time counter)" and "a secret value". The real-time counter value and the secret value do <u>not</u> represent the state of at least one processor. Further, DeBellis fails to disclose the use of any processor state information to generate a string of random bits. Thus, DeBellis fails to disclose the elements of amended claim 32.

Accordingly, for at least these reasons, Applicant respectfully submits that claim 32 is allowable over DeBellis. Given that claims 34-37 depend from claim 32, Applicant respectfully submits that those claims are likewise allowable over DeBellis for at least the reasons discussed above.

Applicant respectfully requests that the §102 rejections be withdrawn.

Conclusion

Claims 1-4, 6-14, 16-32, and 34-37 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 7-13-05

By: Ste Sponsell

Steven R. Sponseller
Reg. No. 39,384
(509) 324-9256